

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-112340

(43)Date of publication of application : 12.04.2002

(51)Int.Cl.

H04Q 7/38  
G06F 15/00  
G06F 17/60  
H04L 9/32

(21)Application number : 2000-297433

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 28.09.2000

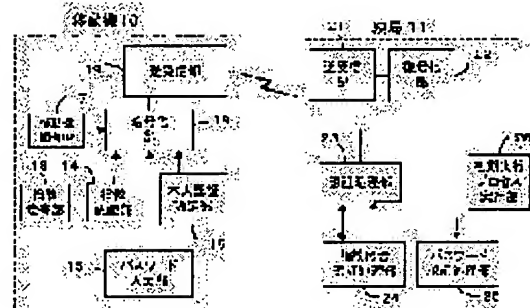
(72)Inventor : AMANO MASAIE  
KIZU SACHIO  
NATSUBORI SHIGEYASU  
IMAI TORU  
TAKAHATA YOSHIKI

## (54) PERSONAL AUTHENTICATION SYSTEM FOR MOBILE DEVICE AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a personal authentication system for a mobile device where a user can freely change an authentication means depending on the purpose of use and then the user can set its satisfied security level by each purpose of use and to provide its method.

SOLUTION: The personal authentication system for mobile device has a plurality of personal authentication means each authenticating that the user of the mobile device is the user and the user sets the cross reference between the personal authentication means and the purpose of use of the mobile device. The system changes the means for authenticating the user depending on the purpose of use of the mobile device based on the cross-reference.



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-112340

(P2002-112340A)

(43) 公開日 平成14年4月12日 (2002. 4. 12)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームト* (参考)
H 0 4 Q 7/38		G 0 6 F 15/00	3 3 0 B 5 B 0 5 U
G 0 6 F 15/00	3 3 0		3 3 0 F 5 B 0 8 U
		17/60	2 2 2 5 J 1 0 4
17/60	2 2 2	H 0 4 B 7/26	1 0 9 S 5 K 0 6 Y
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A

審査請求 未請求 請求項の数12 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願2000-297433 (P2000-297433)

(22) 出願日 平成12年9月28日 (2000. 9. 28)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 天野 真家

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 木津 左千夫

東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内

(74) 代理人 100081732

弁理士 大胡 典夫 (外2名)

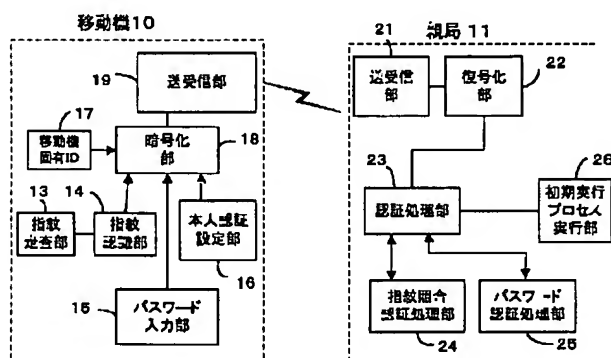
最終頁に続く

(54) 【発明の名称】 移動機の本人認証システム及びその方法

(57) 【要約】

【課題】 使用目的に応じて本人が自由に認証手段を変えることができ、したがって使用目的毎に本人の満足するセキュリティレベルを設定することが可能な、移動機の本人認証システム及びその方法提供すること。

【解決手段】 移動機の利用者が本人であることの認証を行う複数の本人認証手段を有して、これらの本人認証手段と移動機の使用目的との対応関係を本人が設定する。この対応関係に基づき、移動機の使用目的に応じて本人認証の手段を変える。



## 【特許請求の範囲】

【請求項1】 親局と交信することにより、移動機の本人認証を行う認証システムであって、  
移動機の利用者が本人であることの認証を行う複数の本人認証手段と、

この本人認証手段と前記移動機の使用目的との対応関係を本人により設定される認証設定手段と、  
前記本人認証手段による判断のための認証情報を前記移動機から入力される認証情報入力手段と、  
この手段により入力された認証情報と予め記憶されている認証情報を比較し本人であるか否かの確認を行う本人確認手段とを備え、

前記認証設定手段により設定された対応関係に基づき利用者の使用目的に応じて本人認証の手段を変えることを特徴とする、移動機の本人認証システム。

【請求項2】 親局と交信することにより、移動機の本人認証を行う認証システムであって、  
移動機の利用者が本人であることの認証を行う複数の本人認証手段と、

この本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、

前記本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、

前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記親局に送信する認証情報送信手段と、

この手段により送られてきた認証情報を前記親局において予め記憶されている認証情報と比較し本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項3】 親局と交信することにより、移動機の本人認証を行う認証システムであって、  
移動機の利用者が本人であることの認証を行う複数の本人認証手段と、

この本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、

前記本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、

前記認証設定手段により設定されたセキュリティレベルが低い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記移動機において予め記憶されている認証情報と比較し本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項4】 前記複数の本人認証手段は、本人の身体的特徴による認証手段と、本人が作成するパスワードとを含むことを特徴とする請求項1乃至3のいずれか1に

記載の移動機の本人認証システム。

【請求項5】 親局と交信することにより、移動機の本人認証を行う認証システムであって、

本人の身体的特徴に基づいて移動機の利用者が本人であることの認証を行うための第1の本人認証手段と、

本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うための第2の本人認証手段と、

前記第1及び第2の本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、

前記第1及び第2の本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、

前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記親局に送信する認証情報送信手段と、

この手段により送られてきた認証情報を前記親局において予め記憶されている認証情報と比較し前記第1及び第2の本人認証手段により本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項6】 親局と交信することにより、移動機の本人認証を行う認証システムであって、

本人の身体的特徴に基づいて移動機の利用者が本人であることの認証を行うための第1の本人認証手段と、

本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うための第2の本人認証手段と、

前記第1及び第2の本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、

前記第1及び第2の本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、

前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記移動機固有のIDにより暗号化して前記親局に送信する認証情報送信手段と、

この手段により送られてきた認証情報を前記親局において予め記憶されている認証情報と比較し前記第1及び第2の本人認証手段により本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項7】 親局と交信することにより、移動機の本人認証を行う認証システムであって、

指紋により移動機の利用者が本人であることの認証を行うための指紋認証手段と、

本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うためのパスワード認証手段

と、  
 高いセキュリティレベルが要求される前記移動機の使用目的には前記指紋認証手段及び前記パスワード認証手段を用い、低いセキュリティレベルの前記移動機の使用目的には指紋認証手段又はパスワード認証手段を用いるよう本人により設定される認証設定手段と、  
 前記指紋認証手段及びパスワード認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、  
 前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記指紋情報とパスワード情報を前記親局に送信する認証情報送信手段と、  
 この手段により送られてきた指紋情報とパスワード情報を前記親局において予め記憶されている指紋及びパスワードと比較し前記指紋認証手段及び前記パスワード認証手段により本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項8】 親局と交信することにより、移動機の本人認証を行う認証システムであって、  
 指紋により移動機の利用者が本人であることの認証を行うための指紋認証手段と、  
 本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うためのパスワード認証手段と、  
 高いセキュリティレベルが要求される前記移動機の使用目的には前記指紋認証手段及び前記パスワード認証手段を用い、低いセキュリティレベルの前記移動機の使用目的には 指紋認証手段又はパスワード認証手段を用いるよう本人により設定される認証設定手段と、  
 前記指紋認証手段及びパスワード認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、  
 前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記指紋情報とパスワード情報を前記移動機の有する固有のIDにより暗号化して前記親局に送信する認証情報送信手段と、  
 この手段により送られてきた指紋情報とパスワード情報を前記親局において復号化した後、予め記憶されている指紋及びパスワードと比較し前記指紋認証手段及び前記パスワード認証手段により本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システム。

【請求項9】 親局と交信することにより、移動機の本人認証を行う認証システムであって、  
 指紋により移動機の利用者が本人であることの認証を行う指紋認証手段と、  
 この指紋認証手段と前記移動機の作動開始との関係を本

人により設定される認証設定手段と、  
 前記指紋認証手段による判断のための指紋情報を前記移動機から入力される指紋情報入力手段と、  
 この手段により入力された指紋情報と予め記憶されている本人の指紋情報を比較し一致したとき移動機の作動開始を許可する作動開始手段とを備えることを特徴とする、移動機の本人認証システム。

【請求項10】 親局と交信することにより、移動機の本人認証を行う認証方法であって、  
 移動機の利用者が本人であることの認証を行う複数の本人認証方法と前記移動機の使用目的との対応関係を本人により設定される認証設定ステップと、  
 前記複数の本人認証方法による判断のための認証情報を前記移動機から入力される認証情報入力ステップと、  
 このステップにより入力された認証情報と予め記憶されている認証情報を比較し本人であるか否かの確認を行う本人確認ステップとを備え、  
 前記認証設定ステップにより設定された対応関係に基づき利用者の使用目的に応じて本人認証の方法を変えることを特徴とする、移動機の本人認証方法。

【請求項11】 親局と交信することにより、移動機の本人認証を行う認証方法であって、  
 移動機の利用者が本人であることの認証を行う複数の本人認証方法と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定ステップと、  
 前記複数の本人認証方法による判断のための認証情報を前記移動機に入力される認証情報入力ステップと、  
 前記認証設定ステップにより設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力ステップにより入力された認証情報を前記親局に送信する認証情報送信ステップと、  
 このステップにより送られてきた認証情報と比較し本人であるか否かの確認を行う本人確認ステップとを備えて成ることを特徴とする、移動機の本人認証方法。

【請求項12】 親局と交信することにより、移動機の本人認証を行う認証方法であって、  
 高いセキュリティレベルが要求される前記移動機の使用目的には、指紋により移動機の利用者が本人であることの認証を行うための指紋認証方法及び、本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うためのパスワード認証方法を用い、低いセキュリティレベルの前記移動機の使用目的には前記指紋認証方法又は前記パスワード認証方法を用いるよう本人により設定される認証設定ステップと、  
 前記指紋認証方法及びパスワード認証方法による判断のための認証情報を前記移動機に入力される認証情報入力ステップと、  
 前記認証設定ステップにより設定されたセキュリティレ

ベルが高い使用目的に移動機を使用するときは、前記指紋情報とパスワード情報を前記移動機の有する固有のIDにより暗号化して前記親局に送信する認証情報送信ステップと、このステップにより送られてきた指紋情報とパスワード情報を前記親局において復号化した後、予め記憶されている指紋及びパスワードと比較し前記指紋認証方法及び前記パスワード認証方法により本人であるか否かの確認を行う本人確認ステップとを備えて成ることを特徴とする、移動機の本人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、本人認証手段を有する移動機に係り、特に複数の本人認証手段を有する移動機の本人認証システム及びその方法に関する。

【0002】

【従来の技術】従来、定期券を使用するときには本人認証を行わない。したがって、個人が定期券を保持し、改札機が定期券に接触して内容を読むことによるレベルでは不法使用を免れているが、定期券を落した場合不法使用を免れることは困難である。

【0003】また、移動機により銀行為替など簡単な操作で多額の金額が動く操作を行い得る場合、移動機を紛失した場合には、不法使用により極めて深刻な事態が発生する危険性がある。

【0004】通常このような場合、パスワードを用いて個人認証を行っているが、パスワードは考えられる全数を試みることによって破られる危険性が高い。銀行のキャッシュカードでは、パスワードの入力誤りを許容する回数を制限することによって上記のようなあらゆる組み合わせを試みてパスワードを見つけることに対抗しているが、完全とは言い難い。

【0005】一般に、個人認証を厳密に行えば行う程、第三者が不法使用を行うことを防止できるが、本人が行う場合にも厳密な手続を必要とすることになり、非常に煩わしい。反面、本人が簡単に認証できれば、第三者も容易に不法使用ができることになり、二律背反の関係にある。しかし、従来の認証システムではどの使用目的に対してどの認証手段を用いるかは予め固定されており、本人が簡単であってもよいと考えるものが非常に複雑であったり、他方本人が重要視しているものが不法使用される不安を感じるほど認証が簡単であったりすることがある。また、移動機を用いて決済などの行為を行う場合、当該移動機の持ち主が正当な持ち主であること、親局が受信した信号が、その操作権限のある正当な移動機から送られてきたものであることが、保証されないと、移動機の不法使用を許してしまうことになる。

【0006】

【発明が解決しようとする課題】上述のように、従来の認証システムでは、各使用目的毎に認証手段が予め決

っており、ある使用目的に対して本人があつて欲しいと思うセキュリティレベルと認証手段が異なっている場合にも、認証システムを変えることができなかった。

【0007】本発明はこのような、従来の認証システムの問題点に鑑みてなされたもので、使用目的に応じて本人が自由に認証手段を変えることができ、したがって使用目的毎に本人の満足するセキュリティレベルを設定することが可能な、移動機の本人認証システム及びその方法を提供することを目的とする。

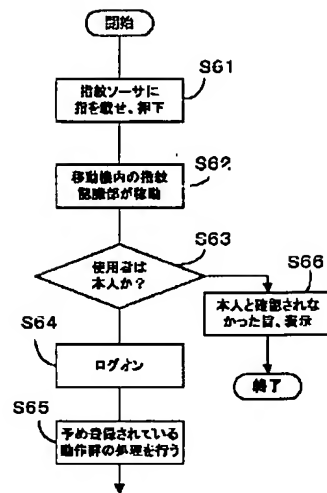
【0008】

【課題を解決するための手段】上記目的を達成するために、本発明の請求項1によれば、親局と交信することにより、移動機の本人認証を行う認証システムであつて、移動機の利用者が本人であることの認証を行う複数の本人認証手段と、この本人認証手段と前記移動機の使用目的との対応関係を本人により設定される認証設定手段と、前記本人認証手段による判断のための認証情報を前記移動機から入力される認証情報入力手段と、この手段により入力された認証情報と予め記憶されている認証情報を比較し本人であるか否かの確認を行う本人確認手段とを備え、前記認証設定手段により設定された対応関係に基づき利用者の使用目的に応じて本人認証の手段を変えることを特徴とする、移動機の本人認証システムを提供する。

【0009】本発明の請求項2によれば、親局と交信することにより、移動機の本人認証を行う認証システムであつて、移動機の利用者が本人であることの認証を行う複数の本人認証手段と、この本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、前記本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、前記認証設定手段により設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記親局に送信する認証情報送信手段と、この手段により送られてきた認証情報を前記親局において予め記憶されている認証情報と比較し本人であるか否かの確認を行う本人確認手段とを備えて成ることを特徴とする、移動機の本人認証システムを提供する。

【0010】本発明の請求項3によれば、親局と交信することにより、移動機の本人認証を行う認証システムであつて、移動機の利用者が本人であることの認証を行う複数の本人認証手段と、この本人認証手段と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定手段と、前記本人認証手段による判断のための認証情報を前記移動機に入力される認証情報入力手段と、前記認証設定手段により設定されたセキュリティレベルが低い使用目的に移動機を使用するときは、前記認証情報入力手段により入力された認証情報を前記移動機において予め記憶されている

【図6】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I

(参考)

H 0 4 L 9/00

6 7 3 C

6 7 3 D

(72)発明者 夏堀 重靖

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 高畠 由彰

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 今井 徹

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

F ターム(参考) 5B055 BB12 CB11 EE03 HA04 HA14

HB02

5B085 AA08 AE03 AE06 AE26

5J104 AA07 KA01 KA16 MA01 NA05

NA43 PA10

5K067 AA32 BB04 DD17 EE02 EE10

EE22 HH22 HH23 HH36 KK15

本人の指紋情報を比較し一致したとき移動機の作動開始を許可する作動開始手段とを備えることを特徴とする、移動機の本人認証システムを提供する。

【0017】本発明の請求項10によれば、親局と交信することにより、移動機の本人認証を行う認証方法であって、移動機の利用者が本人であることの認証を行う複数の本人認証方法と前記移動機の使用目的との対応関係を本人により設定される認証設定ステップと、前記複数の本人認証方法による判断のための認証情報を前記移動機から入力される認証情報入力ステップと、このステップにより入力された認証情報と予め記憶されている認証情報を比較し本人であるか否かの確認を行う本人確認ステップとを備え、前記認証設定ステップにより設定された対応関係に基づき利用者の使用目的に応じて本人認証の方法を変えることを特徴とする、移動機の本人認証方法を提供する。

【0018】本発明の請求項11によれば、親局と交信することにより、移動機の本人認証を行う認証方法であって、移動機の利用者が本人であることの認証を行う複数の本人認証方法と前記移動機の使用目的との対応関係をセキュリティレベルの高低に応じて本人により設定される認証設定ステップと、前記複数の本人認証方法による判断のための認証情報を前記移動機に入力される認証情報入力ステップと、前記認証設定ステップにより設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記認証情報入力ステップにより入力された認証情報を前記親局に送信する認証情報送信ステップと、このステップにより送られてきた認証情報を前記親局において予め記憶されている認証情報と比較し本人であるか否かの確認を行う本人確認ステップとを備えて成ることを特徴とする、移動機の本人認証方法を提供する。

【0019】本発明の請求項12によれば、親局と交信することにより、移動機の本人認証を行う認証方法であって、高いセキュリティレベルが要求される前記移動機の使用目的には、指紋により移動機の利用者が本人であることの認証を行うための指紋認証方法及び、本人が作成するパスワードに基づいて移動機の利用者が本人であることの認証を行うためのパスワード認証方法を用い、低いセキュリティレベルの前記移動機の使用目的には前記指紋認証方法又は前記パスワード認証方法を用いるよう本人により設定される認証設定ステップと、前記指紋認証方法及びパスワード認証方法による判断のための認証情報を前記移動機に入力される認証情報入力ステップと、前記認証設定ステップにより設定されたセキュリティレベルが高い使用目的に移動機を使用するときは、前記指紋情報とパスワード情報を前記移動機の有する固有のIDにより暗号化して前記親局に送信する認証情報送信ステップと、このステップにより送られてきた指紋情報とパスワード情報を前記親局において復号化した後、

予め記憶されている指紋及びパスワードと比較し前記指紋認証方法及び前記パスワード認証方法により本人であるか否かの確認を行う本人確認ステップとを備えて成ることを特徴とする、移動機の本人認証方法を提供する。

【0020】

【発明の実施の形態】以下、本発明の各実施形態について図面を用いて説明する。

【0021】図1に、本発明の一実施形態の移動機における本人認証システムの構成例を示し、図2に親局と移動機の関係を示す。

【0022】図2において、所定範囲内にこの範囲内を移動する複数の移動機10a、10bとの交信を行う親局11が設置されている。親局11は、移動機10a、10bなどと情報の交換を行う前に、それらの移動機を使用している者が本人であることの認証の手続を行う。

【0023】図1において、この移動機の本人認証システム11は、指紋を当接されて指紋を電気信号に変える指紋走査部13とこの電気信号に変えられた指紋を指紋として認識する指紋認識部14と、パスワードを入力するパスワード入力部15と、どの手続にどの本人認証手段を用いるか設定を行う本人認証設定部16と、パスワードや指紋によりなされた情報を移動機の固有ID17により暗号化する暗号化部18と、暗号化された信号を親局11に送信する送受信部19とから成る。

【0024】移動機固有ID17は、移動機に一意的に割り振られているID、例えばSIM(Subscriber Identity Module)番号やMIN(Mobile Identification Number)などであり、これは親局には予め知られている。

【0025】親局11には、移動機から送られてきた信号を受信する送受信部21と、受信した信号をその移動機固有IDで復号化する復号化部22と、移動機で本人認証設定部16で設定された使用目的と認証手段の関係に基づいて信号を送ってきた移動機が本人により使用されていることの認証処理を行う認証処理部23と、具体的に指紋照合により本人を行う指紋照合認証処理部24と、パスワードによる本人認証を行うパスワード認証処理部25と、これらの認証手段により本人であることが確認された後、使用目的に沿った処理がなされる初期実行プロセス実行部26が含まれている。

【0026】本発明の一実施形態における移動機10の外観の例を図3に示す。この移動機は通常の携帯電話やPHSなどであり、前面下部には、文字などを入力する入力ボタン31を有し、前面上部には、入力された文字や受信した情報を表示するための表示画面32が設けられている。

【0027】この移動機30の、通常、使用者が手で保持する側面には、指紋ソーサ33が設けられていて使用者の指紋の情報が取得される。これは移動機の入りスイッチと兼用(あるいは作動開始を意味するログオン)になっている。



【0028】この指紋ソーサ33は図1の指紋走査部13に該当する。指紋ソーサ33は指先くらいの大きさの皿型の軽い凹面形状をしている。このように移動機30の側面の通常使用者が把持する位置に設けられていると、目で指の位置を確認することなく指を当てることができ、認証手段が指紋の場合には、本人認証のための特別の操作が必要でなく、極めて容易に本人認証ができる利点がある。

【0029】即ち、図6に示すように、移動機における本人認証は、ステップS61で指紋ソーサ33に指を載せて押下すると、ステップS62で移動機内の指紋認識部（図示せず）が稼動し、ステップS63で本人であるかどうか確認され、本人であるとステップS64でログオンし、ステップS65で予め登録されている動作群の処理を行う。ステップS63で指紋が予め登録されている指紋と一致しないと、ステップS66その旨表示される。

【0030】指紋ソーサ33は、凹面の他、平面で感触の異なる材料により形成して、指先で指紋ソーサの位置がすぐ判別できるようにしてもよい。

【0031】移動機10の本人認証設定部16には、使用者によって移動機10が使われる目的とその使用目的の場合の本人認証の手段が対応して設定され記憶される。この情報は予め暗号化部18において、移動機固有ID17によって暗号化され、送受信部19を介して親局11に送られている。

【0032】この移動機を使用する者は、例えば図4に示すように、定期券として使用するときには指紋を用いることとし、銀行決済の場合には指紋とパスワード(PW)を認証手段として使用するよう設定する。

【0033】次に、本発明の上記実施形態について、定期券として移動機を使う場合の動作について図5を用いて説明する。

【0034】移動機10aを使用する者が、ログインしてから移動機の使用目的を選択する。この場合、図4に示した内容は親局に既に送られているので、使用者が使用目的を定期券とすると、指紋のみが本人認証に使われることになる。

【0035】移動機10aから、指紋走査部13及び指紋認識部14にて得られた、使用者の指紋が移動機固有ID17により暗号化されて送受信部19から親局に送られる。

【0036】親局では、ステップS51で移動機の使用目的をまず検知する。次にステップS52において、認証手段指紋認証が必要かどうか調べられる。定期券として移動機を用いる場合には、指紋が本人認証の手段であるから、ステップS53に移動し、指紋による本人認証の手続を実行する。即ち、親局は移動機10aから送られてきた信号を、送受信部21で受信し復号化部22において、移動機固有ID17で復号化する。復号化され

た指紋情報は認証処理部23を介して指紋認証処理部24に送られ、移動機固有IDによって特定される移動機の所有者の予め記憶されていた指紋と今度送られてきた指紋の情報が比較される。

【0037】尚、ステップS52において、指紋認証が必要でない場合には、ステップS54でパスワード(PW)により本人認証がなされる。

【0038】上記のように本人認証手続がなされた後、ステップS55において、本人であることが確認されたか、調べられる。上記のようにして指紋照合認証処理部24において比較の結果が一致すれば、該当移動機10aの所有者と指紋が一致したことになり、本人と確認されたことになる。

【0039】次に、ステップS56で更にパスワードによる認証が必要か否か調べられる。定期券の場合、図4に示したように指紋による認証のみであるから、ステップS56では、NoになりステップS57に移り、使用目的に処理、即ち定期券としての処理がなされ、終われば終了することになる。

【0040】ステップS55で、送られてきた指紋の情報が、移動機10aの所有者の指紋の情報と一致しなかったら、本人であることが確認されなかったことになるので、ステップS58でその旨の情報を当該移動機10aに送って、その画面上「本人であることが確認されませんでした」などの表示を行い、処理を終了する。

【0041】このように、定期券の場合に指紋を用いれば、個人の特有の指紋によって簡単にしかも高速に本人であることの認証を行い得る利点がある。

【0042】移動機での指紋による本人認証で、初期設定によって定期券情報が発せられるようにすることができる。この初期設定では移動機での指紋による本人認証で機動するプロセスを単数又は複数設定することができる。移動機での指紋による本人認証で、移動機へのログインを許可するだけに設定することも可能であり、続いて他の定期券ボタンのようなものを押すようにしてもよい。

【0043】上記実施形態では、指紋ソーサに指を置き、軽く押すなどの何らかの操作を加えることによって、あるいはキャパシタセンサ、圧力センサ、などにより、指が載せられたことを検知することによって、指紋認識部が起動し指紋認識が発せられる。指紋が認識されることによって本人認証が完了し、移動機から定期券情報が発せられ、改札機と情報を交換することによって通り抜けることができる。

【0044】次に、移動機11aを銀行決済に使用する場合の認証手続について説明する。

【0045】図4によれば、銀行決済の場合には、本人認証の手段として指紋とパスワードを用いる。移動機10aを使用する者が、指紋によるログインを行う。即ち、指紋照合による本人認証を移動機内で行い、移動機



10aの使用者の指紋として予め記憶されている指紋と、指紋が一致するかどうか調べて一致している場合にのみログインを許す。

【0046】移動機10aでは、使用目的として銀行決済を選択する。次に移動機10aの指紋走査部13により使用者の指紋が取られ指紋認識部14にて指紋として認識された後、指紋情報として、暗号化部18にて移動機固有IDにより暗号化され送受信部19を介して親局11に送る。また、移動機10のパスワード入力部15からも使用者が入力したパスワードが暗号化部18で暗号化され、送受信部19を介して親局11に送られる。

【0047】親局11では、ステップS51で移動機10aの使用目的即ち、銀行決済であることを検知する。次にステップS52で認証手段として指紋認証が必要か調べられる。図4に示したように銀行決済の場合の認証手段は指紋とパスワードであるので、ステップSではYesとなりステップS53で指紋による認証手続がなされる。

【0048】この指紋による認証手続は、上述の場合と同じなので、詳しくは説明しないが、指紋認証処理部23において送られてきた指紋情報を、予め記憶されている本人の指紋情報と比較し一致するかどうか調べられる。

【0049】次に、ステップS55で本人であることが確認されたかどうか調べられる。上記指紋情報が一致すれば、本人であることが確認されたことになる。ステップS55でYesとなると、ステップS56に移り、更に認証が必要かどうか調べられる。銀行決済の場合、指紋のほかにパスワードでも認証が必要なので、ステップS56ではYesとなり、ステップS54に戻りパスワードによる本人認証の手続が行われる。

【0050】次にステップS55で、パスワードが予め移動機10aの所有者により登録されたパスワードと一致するかどうか調べられ、一致すればYesとなり、再びステップS56に進む。

【0051】今の場合、パスワードを1つと仮定すると、ステップS56ではNoとなり、ステップS57に移って使用目的、即ち銀行決済の処理がなされる。銀行決済の手続が完了すれば、終了する。

【0052】なお、指紋による本人認証手続又はパスワードによる本人認証手続において、指紋あるいはパスワードが一致しなければ、ステップS58に移り、移動機10aに情報を送り、本人であることが確認できなかった旨、移動機の表示画面に表示される。

【0053】この実施形態によれば、銀行決済のような重大な操作を移動機から行う場合、最低でも性質の異なる2段階の認証過程を経ている。まず、指紋による認証を行うが、指紋照合による認証で移動機にログインする。次にメニューから銀行決済のプロセスに進みその中で再度親局による指紋認証とパスワードによる本人認証

を行う。親局による指紋認証は指紋を移動機に固有のIDをキーにして暗号化したものを用いるので、本人認証だけでなく移動機の認証を行うこともできる。したがって、なんらかの方法で指紋を偽造することができたとしても、固有の移動機からアクセスしない限り認証されない。

【0054】また、暗号化されたコードが乗っている電波を傍受し何らかの方法で同じパターンの電波を他の移動機から送信することができたとしてもその移動機固有のIDは本来のIDと異なるので、認証されない。更に、認証を行う際のパスワードも移動機の固有IDをキーとして暗号化されているので、パスワード自体を傍受することも暗号化された電波のパターン自体を認証することも不可能になる。

【0055】上記実施形態では、パスワードは1つだけ用いていた。しかし、2つ以上のパスワードを用いるようにすることもできる。

【0056】上記実施形態では、指紋情報を移動機から親局に送り、親局において指紋情報の比較・照合を行っていた。しかし、移動機に指紋情報を比較する指紋照合認証処理部を設けて親局に送ることなく、移動機内で指紋による本人認証を行うことも可能である。このようにすれば、比較的速く本人認証ができる利点がある。

【0057】また、使用目的によって、認証のための情報を親局に送り親局で本人認証の手続を取るか、移動機内で、本人認証の手続を取るか分けることができる。例えば、移動機を定期券として使用する場合には、指紋を用いて移動機内で本人認証を行い、銀行決済の場合には、指紋やパスワードの情報を親局に送って親局で本人認証を行い、本人であることの確認結果を移動機に送るようにすることができる。このようにすれば、定期券として使う場合には速く認証手続が行え、銀行決済の場合には本人認証を厳密に行うことができ、極めてセキュリティの高いシステムを構築することができる。

【0058】また、例えば、指紋による認証については移動機において行い、パスワードによる認証については親局にて行うなど、移動機で行う認証手段と、親局において行う認証手段を分けることもできる。

【0059】また、上述の場合には、指紋を用いる場合について説明したが、指紋に限らず顔の形状など個人の身体的特徴を用いることができる。上述のように、移動機固有のIDを用いて暗号化して親局に送信し、親局で本人認証の手続を行うようにすると、異なる移動機では別の固有IDにより暗号化されることになり、親局ではその移動機からの情報として適正に復号化されない。即ち、認証情報を送っても、暗号化したキーがその移動機特有のIDでないと、認証サーバは受け付けない。たとえIDが発見されてそれにより暗号化しても送信されてきた移動機のIDとは異なるので、認証サーバはこれを「本機」ではないと認識し、拒否できる。同じIDの移

動機は移動網内に2台は存在し得ないので、これだけは偽造できない。

【0060】

【発明の効果】本発明によれば、移動機の利用者によって本人認証の手段を変えることができ、自分の必要と考えるようにセキュリティレベルを設定できる。

【図面の簡単な説明】

【図1】本発明の一実施形態の構成例を示す図。

【図2】本発明における移動機と親局の関係を示す図。

【図3】本発明の一実施形態における移動機の外観を示す図。

【図4】本発明の一実施形態において移動機の使用目的と認証手段の対応関係の例を示す図。

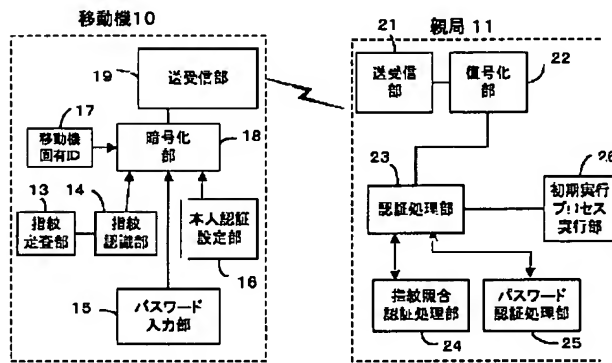
【図5】本発明の一実施形態における本人認証の処理の流れを示す図。

【図6】本発明の一実施形態の移動機におけるログオン時の処理の流れを示す図。

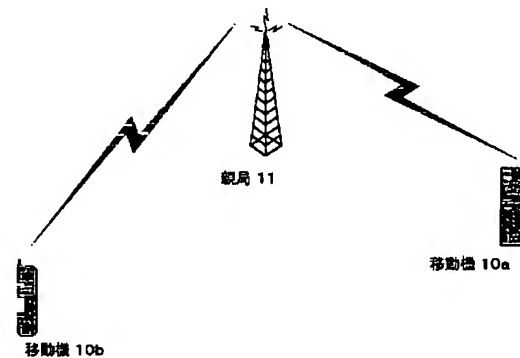
【符号の説明】

10, 10a, 10b・・・移動機、11・・・親局、13・・・指紋走査部、14・・・指紋認識部、15・・・パスワード入力部、16・・・本人認証設定部、17・・・移動機固有ID、18・・・暗号化部、19, 21・・・送受信部、22・・・復号化部、23・・・認証処理部、24・・・指紋照合認証処理部、25・・・パスワード認証処理部、26・・・初期実行プロセス実行部。

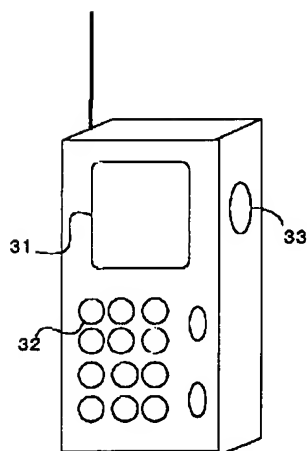
【図1】



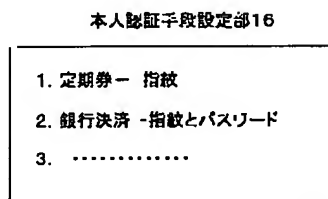
【図2】



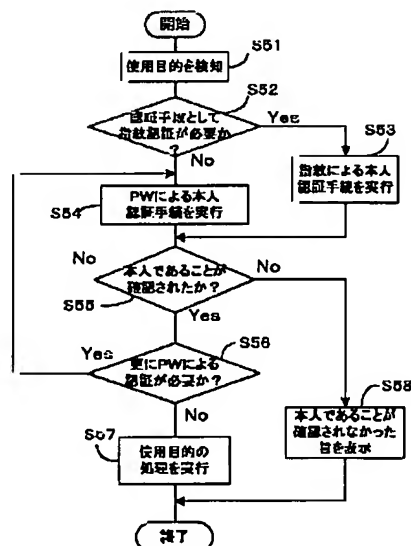
【図3】



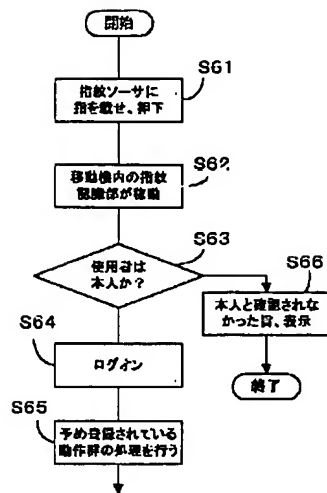
【図4】



【図5】



【図6】




---

フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I

(参考)

H 0 4 L 9/00

6 7 3 C

6 7 3 D

(72)発明者 夏堀 重靖

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 高畠 由彰

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(72)発明者 今井 徹

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

Fターム(参考) 5B055 BB12 CB11 EE03 HA04 HA14

HB02

5B085 AA08 AE03 AE06 AE26

5J104 AA07 KA01 KA16 MA01 NA05

NA43 PA10

5K067 AA32 BB04 DD17 EE02 EE10

EE22 HH22 HH23 HH36 KK15